Claims

What is claimed:

1. A data processing system for generating at least one unique base key comprising a cryptographic device including at least one master group key, at least one security token including a unique identifier, and communication means for exchanging data between said cryptographic device and said token, wherein
   - said cryptographic device includes logic operator means combining said at least one master group key with said unique identifier received from said token through said communication means, producing said at least one unique base key,
   - said at least one security token includes data storage means for storing said at least one unique base key and cryptographic means using said stored at least one unique base key

2. The system according to claim 1, wherein said logic operator means includes an exclusive OR bit-wise operator means.

3. The system according to claim 2, wherein said unique identifier and said master group key are used as operands by said exclusive OR bit-wise operator means forming said at least one base key.

4. The system according to claim 1 further including message digest function means for digesting said unique identifier before operation by said logic operator means.

5. A method of generating at least one unique base key comprising the steps of
   - generating a master group key by a cryptographic device,
   - receiving a unique identifier from a first security token by said cryptographic device,
   - performing a logic operation using said unique identifier and said master group key as operands producing said at least one unique base,
   - operatively injecting said at least one unique base key into said first security token,
   - repeating said steps for at least a second security token.

6. The method according to claim 5, further comprising the steps of digesting said unique identifier using a message digest function.

7. The method according to claim 6, wherein said logic operation includes an exclusive OR bit-wise operation.

8. A system for performing symmetric keys based mutual authentications between at least two security tokens comprising:

a first secure token including a first unique identifier, a first unique base key which is a function of a master key and of said first unique identifier, first cryptography means, and first memory storage means;

a second security token including a second unique identifier, a second unique base key which is a function of said master key and of said second unique identifier, and second cryptography means compatible with said first cryptography means, second memory storage means and

communication means for exchanging data between said first and second secure tokens, wherein

said first secure token comprises first logic operator means for processing said first unique base key and said second unique identifier received from said second security token, producing a first composite group key,

said second secure token comprises second logic operator means for processing said second unique base key and said first unique identifier received from said first security token, producing a second composite group key,

said first and second composite group keys being equal.

9. The system according to claim 8 wherein said second unique identifier processed by said first logic operator means is a message digest of said second unique identifier, said first security token comprising first message digest function means for digesting said second unique identifier received using said communications means from said second security token.

10. The system according to claim 9 wherein said first unique identifier processed by said second logic operator means is a message digest of said first unique identifier, said second security token comprising second message digest function means for digesting said first unique identifier received using said communications means from said first security token.

11. The system according to claim 10 wherein said first logic operator means comprises a first exclusive OR bit-wise operator, said message digest of said second unique identifier and said first unique base key being used as operands by said first exclusive OR bit-wise operator, producing said first composite group key which is stored using said first memory storage means.

12. The system according to claim 11 wherein said second logic operator means comprises a second exclusive OR bit-wise operator, said message digest of said first unique identifier and said second unique base key being used as operands by said second exclusive OR bit-wise operator, producing said second composite group key which is stored using said second memory storage means.

13. The system according to claim 12 wherein said first security token comprises first random number generating means for generating a first random number, said first random number being stored using said first memory storage means, said first cryptographic means encrypting said first random number with said first composite group key producing a first cryptogram.

14. The system according to claim 13 wherein said second security token comprises second random number generating means for generating a second random number, said second random number being stored using said second memory storage means, said second cryptographic means encrypting said second random number with said second composite group key producing a second cryptogram.

15. The system according to claim 14 wherein said first cryptogram is sent to said second security token using said communications means and decrypted using said second composite group key and said second cryptographic means, producing a first random number result.

16. The system according to claim 15 wherein said second cryptogram is sent to said first security token using said communications means and decrypted using said first composite group key and said first cryptographic means, producing a second random number result.

17. The system according to claim 16 wherein said first random number result is sent to said first security token using said communications means, said first security token comprising first comparing means for comparing said first random number result to said first random number retrieved using said first memory storage means..

18. The system according to claim 17 wherein said second random number result is sent using said communications means to said second security token, said second security token comprising second comparing means for comparing said second random number result to said second random number retrieved using said second memory storage means.

19. The system according to claim 17 wherein a match between said first random number result and said first random number authenticates said second security token to said first security token.

20. The system according to claim 18 wherein a match between said second random number result and said second random number authenticates said first security token to said second security token.

21. The system according to claim 8 wherein said first cryptographic means and said second cryptographic means includes at least one common symmetric cryptographic algorithm.

22. A method for performing mutual authentications between a first security token and a second security token comprising:

sending a first unique identifier from a first security token to a second security token,

sending a second unique identifier from said second security token to a said first security token,

digesting said second unique identifier by said first security token using a message digest function mutually installed in said first and said second security tokens producing a second digest result,

digesting said first unique identifier by said second security token using said message digest function producing a first digest result,

performing an exclusive OR bit-wise operation by said second security token using said second digest result and a second unique base key as operands, producing a second composite group key,

performing an exclusive OR bit-wise operation by said first security token using said first digest result and a second unique base key as operands, producing a first composite group key,

generating a first random number by said first security token, storing a copy of said first random number and encrypting said first random number using said first composite group key and a mutually shared cryptographic algorithm, producing a first cryptogram,

generating a second random number by said second security token, storing a copy of said second random number and encrypting said second random number using said second composite group key and said mutually shared cryptographic algorithm, producing a second cryptogram,

sending said first cryptogram from said first security token to said second security token,

sending said second cryptogram from said second security token to said first security token,

receiving and decrypting said first cryptogram using said second composite group key and said mutually shared cryptographic algorithm by said second security token producing a first random number result,

receiving and decrypting said second cryptogram using said first composite group key and said mutually shared cryptographic algorithm by said first security token producing a second random number result,

sending said first random number result from said second security token to said first security token,

sending said second random number result from said first security token to said second security token,

receiving said first random number result by said first security token, retrieving said copy of said first random number from memory and comparing said first random number result to said copy of said first random number,

receiving said second random number result by said second security token, retrieving said copy of said second random number from memory and comparing said second random number result to said copy of said second random number,

authenticating said second security token to said first security token if said first random number result matches said copy of said first random number,

authenticating said first security token to said second security token if said second random number result matches said copy of said second random number.

23. The method according to claim 22, wherein said mutually shared cryptographic algorithm is a symmetric algorithm.

24. A program storage device readable by a machine, tangibly embodying a program of instructions executable by said machine to perform the method steps of claim 5 or 22.